Totally indefinite Euclidean quaternion fields

Jean-Paul Cerri, Jérôme Chaubert, Pierre Lezowski

Totally indefinite Euclidean quaternion fields

Jean-Paul Cerri
Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France
CNRS, IMB, UMR 5251, F-33400 Talence, France
INRIA LFANT, F-33400 Talence, France
e-mail: jean-paul.cerri@math.u-bordeaux.fr

Jérôme Chaubert
rue du talent
1042 Malapalud, Suisse
e-mail: jerome.chaubert@gmail.com

Pierre Lezowski
INRIA LFANT, F-33400 Talence, France
CNRS, IMB, UMR 5251, F-33400 Talence, France
Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France
e-mail: pierre.lezowski@math.u-bordeaux.fr

Abstract

We study the Euclidean property for totally indefinite quaternion fields. In particular, we establish the complete list of norm-Euclidean such fields over imaginary quadratic number fields. This enables us to exhibit an example which gives a negative answer to a question asked by Eichler. The proofs are both theoretical and algorithmic.

1 Introduction

Quaternion fields are special cases of central division algebras. Let us recall that such an algebra F is a 4-dimensional algebra over a number field K with basis $(1, i, j, k)$ such that $i^2 = a$, $j^2 = b$ and $k = ij = -ji$, where a, b are non-zero elements of K. This

2010 *Mathematics Subject Classification*: Primary 13F07; Secondary 11Y40, 16H05, 16H10
Key words and phrases: Totally indefinite quaternion field; Euclidean order; norm-Euclidean order.

algebra is denoted by $\left(\frac{a,b}{K}\right)$. Let $w = x+yi+zj+tk \in \left(\frac{a,b}{K}\right)$, where $x, y, z, t \in K$. We denote by $\overline{w}$ the image of w by the canonical involution of $\left(\frac{a,b}{K}\right)$, which is defined by $\overline{w} = x - yi - zj - tk$, and by $\mathrm{nrd}_{F/K}(w) = w\overline{w}$ its reduced norm. The algebra $\left(\frac{a,b}{K}\right)$ is a division algebra if and only if the quadratic form $\mathrm{nrd}_{F/K}(x + yi + zj + tk) = x^2 - ay^2 - bz^2 + abt^2$ represents zero on K only trivially. In this case, we say that $\left(\frac{a,b}{K}\right)$ is a quaternion field. Throughout this paper, F will be a quaternion field over a number field K. We will denote by $\mathbb{Z}_K$ the ring of integers of K, by $\mathbb{Z}_K^\times$ its unit group and by $N_{K/\mathbb{Q}}$ the norm form. We will also use $N_{K/\mathbb{Q}}$ for the norm of an ideal (if I is a nonzero ideal of $\mathbb{Z}_K$, $N_{K/\mathbb{Q}}(I) = |\mathbb{Z}_K/I|$) and $\mathrm{nrd}_{F/K}$ for the reduced norm of an ideal (if J is an ideal of F, $\mathrm{nrd}_{F/K}(J)$ is the ideal of K generated by the $\mathrm{nrd}_{F/K}(x)$, $x \in J$).

Definition 1.1. Let Λ be an order of F. We say that Λ is *right-Euclidean* if and only if there exist a well-ordered set W and a map $\Phi : \Lambda \longrightarrow W$ such that for every $(a, b) \in \Lambda \times \Lambda \setminus \{0\}$ there exists some $q \in \Lambda$ satisfying

$$\Phi(a - bq) < \Phi(b). \tag{1}$$

We will also say that Φ is a *right-Euclidean stathm* for Λ.

Let us denote by $N : F \longrightarrow \mathbb{Q}_{\geq 0}$ the absolute value of the reduced norm map $\mathrm{nrd}_{F/\mathbb{Q}} : F \longrightarrow \mathbb{Q}$ defined by $\mathrm{nrd}_{F/\mathbb{Q}} = N_{K/\mathbb{Q}} \circ \mathrm{nrd}_{F/K}$. The map N is multiplicative and for any order Λ of F, it satisfies $N(\Lambda) \subseteq \mathbb{Z}_{\geq 0}$. So N, with $W = \mathbb{Z}_{\geq 0}$, is a natural and practical candidate for checking whether Λ is right-Euclidean, which leads to the following, more precise definition.

Definition 1.2. An order Λ of F is *right-norm-Euclidean* if for any $(a, b) \in \Lambda \times \Lambda \setminus \{0\}$, there exists some $q \in \Lambda$ such that

$$N(a - bq) < N(b). \tag{2}$$

We can define similarly *left-Euclidean orders* and *left-norm-Euclidean orders* by replacing bq by qb in (1) and (2). In fact, these two notions are equivalent, which allows to speak of Euclidean and norm-Euclidean orders (see [3]). Moreover, if F admits a Euclidean (repectively norm-Euclidean) order Λ, then Λ is maximal and every maximal order of F is also Euclidean (respectively norm-Euclidean), which enables us to speak of Euclidean (respectively norm-Euclidean) quaternion fields: quaternion fields admiting a Euclidean (respectively norm-Euclidean) maximal order. All these considerations are developed in [3] and will be recalled in Section 2.

Our main results are the following theorems which deal with totally indefinite quaternion fields, i.e. quaternion fields in which no infinite place is ramified.

Theorem 3.4. *Let F be a totally indefinite quaternion field over a number field K. Then the following statements hold.*

(i) *If K is Euclidean, then F is Euclidean;*

(ii) *If K is norm-Euclidean, then F is norm-Euclidean;*

(iii) *If the class number of K is equal to 1, then for any maximal order Λ of F, we have $M(\Lambda) \leq M(K)$.*

We refer the reader to Section 2 for the definitions of the Euclidean minima $M(\Lambda)$ and $M(K)$. This result will enable us to find an example of Euclidean quaternion field which is not norm-Euclidean (see Proposition 3.8).

Eichler [6, Section IV] had already studied a variation of the norm-Euclidean property for quaternion fields satisfying the so-called *Eichler condition*[1] (which is satisfied by any totally indefinite quaternion field). He proved a statement similar to (ii), but his proof (as others in the literature) seems to be incomplete. See Section 3 for details.

Theorem 4.1. *Let $K = \mathbb{Q}(\sqrt{-d})$ (where d is a squarefree positive integer) be an imaginary quadratic number field. Let F be a quaternion field over K. Then F is norm-Euclidean if and only if $d \in \{1, 2, 3, 7, 11\}$ or $F = \left(\frac{-2,-5}{\mathbb{Q}(\sqrt{-19})}\right)$.*

Eichler asked a question that can be reformulated in our context as follows. Let F be a totally indefinite[2] quaternion field over a number field K. Let us suppose that F is norm-Euclidean. Does this imply that K is norm-Euclidean? The last quaternion field of Theorem 4.1 provides a negative answer to this question. It is norm-Euclidean while the field $\mathbb{Q}(\sqrt{-19})$ is not norm-Euclidean, and even not Euclidean.

The organization of the paper is as follows. In Section 2, we give basic definitions and recall some properties of totally indefinite quaternion fields and Euclidean quaternion fields. Then Sections 3 and 4 are respectively devoted to proving Theorem 3.4 and Theorem 4.1.

2 First definitions

2.1 Orders, ideals

We first recall some definitions and basic properties. The reader may refer to [5], [10] and [11] for more details. Let v be a place of K and K_v be the completion of K at v.

[1] A quaternion field F over a number field K satisfies the Eichler condition if there exists at least one infinite place of K which is not ramified in F.

[2] Actually, he only asked for F to satisfy the *Eichler condition*, which is looser in general. When K is an imaginary quadratic field, F is totally indefinite and as a consequence, it satisfies the Eichler condition.

We say that v is *ramified* in F if $F_v = F \otimes_K K_v$ is a skew field. An infinite place of K which is ramified in F is necessarily real. The set of places (finite and infinite) which are ramified in F is nonempty (since F is a field), of even cardinality and uniquely characterizes F up to K-algebra isomorphism. If no infinite place is ramified, we say that F is *totally indefinite*. As a consequence, if K is totally complex, any quaternion field over K is totally indefinite. In this case, the number of finite places of K which ramify in F is a positive even number.

An *ideal* I of a quaternion field F is a full $\mathbb{Z}_K$-lattice in F, i.e. such that $KI = F$. An *order* of F is an ideal which is also a subring of F. Equivalently, an order Λ of F is a subring of F containing $\mathbb{Z}_K$ such that $K\Lambda = F$ and whose elements are integral over $\mathbb{Z}_K$. An order is *maximal* if it is not properly contained in another order. An ideal I defines two orders, its *right order* and its *left order* respectively given by: $O_r(I) = \{x \in F;\ Ix \subseteq I\}$ and $O_l(I) = \{x \in F;\ xI \subseteq I\}$.

Two ideals I, J are left-equivalent if there exists some $x \in F \setminus \{0\}$ such that $I = xJ$. The classes of ideals with right order Λ are called the right classes of Λ. We define in the same way the left classes of Λ. If Λ is a maximal order of F, the number of right classes of Λ is finite and equal to the number of left classes of Λ. Moreover this number is independent of the choice of Λ. It is called the *class number* of F and we will denote it by h_F.

Two orders Λ and Λ' of F are of the same type (or conjugate) if there exists some $x \in F \setminus \{0\}$ such that $\Lambda' = x^{-1}\Lambda x$. This defines an equivalence relation over the set of maximal orders in F. The number of classes for this relation in the set of maximal orders is called the *type number* of F and we will denote it by t_F. We have $t_F \leq h_F$.

An ideal I is *two-sided* if $O_r(I) = O_l(I)$, *normal* if both $O_r(I)$ and $O_l(I)$ are maximal orders, *integral* if it is normal and if $I \subseteq O_r(I)$. In the latter case, we also have $I \subseteq O_l(I)$. For instance, if Λ is a maximal order and if $b \in \Lambda \setminus \{0\}$, then $b\Lambda$ is an integral ideal with right order Λ and left order its conjugate $b\Lambda b^{-1}$.

Let Λ be a maximal order. A *prime ideal* $\mathfrak{P}$ of Λ is a proper integral two-sided ideal with right order Λ such that for every pair of two-sided ideals S, T, with the same properties, if $ST \subseteq \mathfrak{P}$ then S or $T \subseteq \mathfrak{P}$. For every prime ideal $\mathfrak{P}$ of a maximal order Λ, there exists a unique prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ such that $\mathfrak{p} \subseteq \mathfrak{P}$ and we have $\mathfrak{p} = \mathfrak{P} \cap \mathbb{Z}_K$. Conversely, if Λ is a maximal order, for every prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$, there exists a unique prime ideal of Λ such that $\mathfrak{p} \subseteq \mathfrak{P}$. With this notation, if the prime $\mathfrak{p}$ is ramified in F, then $\mathfrak{p}\Lambda = \mathfrak{P}^2$.

A *maximal* ideal $\mathfrak{N}$ is a maximal element in the set of proper integral ideals with right order $O_r(\mathfrak{N})$. In this case, $\mathfrak{N}$ is also maximal in the set of proper integral ideals with left order $O_l(\mathfrak{N})$.

Remark 2.1. Assume that Λ is a maximal order and that $\mathfrak{N}$ is a maximal ideal with

right order Λ. In contrast to the commutative case, we can find $x, y \in \Lambda$ such that $xy \in \mathfrak{N}$ but neither x nor y belongs to $\mathfrak{N}$. For instance let us take $F = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\Lambda = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + \frac{1+i+j+k}{2}\mathbb{Z}$, respectively the Hamilton quaternion field and the Hurwitz quaternion ring. Set $\alpha = 1+i+j$ and $\mathfrak{N} = \alpha\Lambda$, which is a maximal ideal with right order Λ. Then $x = 1+i+k$ and $y = \overline{x}$ satisfy $xy = 3 \in \mathfrak{N}$ and neither $x \in \mathfrak{N}$ nor $y \in \mathfrak{N}$.

For every maximal ideal $\mathfrak{N}$ with right maximal order Λ, there is a unique prime ideal $\mathfrak{P}$ of Λ such that $\mathfrak{P} \subseteq \mathfrak{N}$ and we have $\mathfrak{P} = \{x \in \Lambda;\ \Lambda x \subseteq \mathfrak{N}\}$. Then, with the previous notation, we have $\mathfrak{N} \cap \mathbb{Z}_K = \mathfrak{P} \cap \mathbb{Z}_K = \mathfrak{p}$ and $\mathrm{nrd}_{F/K}(\mathfrak{N}) = \mathfrak{p}$.

A *proper product* of ideals is a product $N_1 \cdots N_l$ where for every $1 \leq i \leq l-1$, $\mathcal{O}_r(N_i) = \mathcal{O}_l(N_{i+1})$. Every proper integral ideal I admits a decomposition into a *proper product* of maximal ideals $I = \mathfrak{N}_1 \cdots \mathfrak{N}_l$ where $O_l(I) = O_l(\mathfrak{N}_1)$ and $O_r(I) = O_r(\mathfrak{N}_l)$ (see [10, Theorem 22.18]). Then, as seen in [3, Lemma 2.2], we have

$$\mathrm{nrd}_{F/K}(I) = \mathrm{nrd}_{F/K}(\mathfrak{N}_1) \cdots \mathrm{nrd}_{F/K}(\mathfrak{N}_l).$$

Lemma 2.2. *Let Λ be a maximal order of F and let $\mathfrak{p}$ be a nonzero prime ideal of $\mathbb{Z}_K$.*

(i) *If $\mathfrak{p}$ is ramified in F, there exists a unique maximal ideal $\mathfrak{N}$ of F such that $\mathfrak{p} \subseteq \mathfrak{N}$. Moreover, $\mathfrak{N}$ is two-sided.*

(ii) *Let $x \in \Lambda$ and $y \in \mathfrak{p}\Lambda$, then $\mathrm{nrd}_{F/K}(x+y) = \mathrm{nrd}_{F/K}(x) \bmod \mathfrak{p}$.*

(iii) *Suppose that $a \in \Lambda \setminus \{0\}$ is such that $\mathrm{nrd}_{F/K}(a) \in \mathfrak{p}$. Then there exists a maximal ideal $\mathfrak{N}$ with right order Λ such that $a \in \mathfrak{N}$ and $\mathfrak{N} \cap \mathbb{Z}_K = \mathfrak{p}$.*

Proof. (i) See [3, Lemma 2.2].

(ii) There exist a positive integer r, $(p_j)_{1\leq j\leq r} \in \mathfrak{p}^r$, and $(\lambda_j)_{1\leq j\leq r} \in \Lambda^r$ such that $y = \sum_{j=1}^r p_j\lambda_j$. We compute $\mathrm{nrd}_{F/K}(x+y) = \mathrm{nrd}_{F/K}(x)+\mathrm{nrd}_{F/K}(y)+\mathrm{trd}_{F/K}(x\overline{y})$. First,

$$\begin{aligned}\mathrm{nrd}_{F/K}(y) &= \sum_{1\leq j<k\leq r} \mathrm{trd}_{F/K}(p_j\lambda_j\overline{p_k\lambda_k}) + \sum_{j=1}^r \mathrm{nrd}_{F/K}(p_j\lambda_j)\\ &= \sum_{1\leq j<k\leq r} p_jp_k\mathrm{trd}_{F/K}(\lambda_j\overline{\lambda_k}) + \sum_{j=1}^r p_j^2\mathrm{nrd}_{F/K}(\lambda_j).\end{aligned}$$

That proves that $\mathrm{nrd}_{F/K}(y) \in \mathfrak{p}$. Likewise,

$$\mathrm{trd}_{F/K}(x\overline{y}) = \sum_{j=1}^r \mathrm{trd}_{F/K}(x\overline{\lambda_j})p_j \in \mathfrak{p}.$$

(iii) Consider the integral ideal $I = a\Lambda + \mathfrak{p}\Lambda$. Its right order is Λ. Assuming $I \subsetneq \Lambda$, there exists a maximal ideal $\mathfrak{N}$ with right order Λ containing I. As $\mathfrak{p}$ is included in $\mathfrak{N}$, we have $\mathfrak{N} \cap \mathbb{Z}_K = \mathfrak{p}$. By construction, we also have $a \in \mathfrak{N}$.

It remains to prove that $I \subsetneq \Lambda$. Let us assume that $I = \Lambda$. Then there exist $\lambda \in \Lambda$ and $\mu \in \mathfrak{p}\Lambda$ such that

$$1 = a\lambda + \mu.$$

But then $1 = \mathrm{nrd}_{F/K}(a\lambda + \mu) = \mathrm{nrd}_{F/K}(a)\mathrm{nrd}_{F/K}(\lambda) \bmod \mathfrak{p}$ thanks to (ii). As $\mathrm{nrd}_{F/K}(a) \in \mathfrak{p}$, this proves that $1 \in \mathfrak{p}$, which is obviously false. Thus, $I \subsetneq \Lambda$.

□

Lemma 2.3. *Let Λ be a maximal order of F. Then, for any a, $b \in \Lambda$ such that $a\Lambda + b\Lambda = \Lambda$, there exists $c \in \Lambda$ such that $\mathrm{nrd}_{F/K}(a + bc)$ and $\mathrm{nrd}_{F/K}(b)$ are coprime*[3]*.*

Such a lemma was stated by Eichler and used without a proof ([6, p. 241]). Vignéras gave an unconvincing proof of it ([11, p. 91])[4].

Remark 2.4. If $h_F = 1$, we can obtain a similar decomposition, even without the assumption that $a\Lambda + b\Lambda = \Lambda$. Indeed, as $a\Lambda + b\Lambda$ is an ideal with right order Λ and $h_F = 1$, there exists a $\mu \in \Lambda$ such that $a\Lambda + b\Lambda = \mu\Lambda$. Then we can consider $\mu^{-1}a$ and $\mu^{-1}b$, which satisfy the hypotheses of the lemma. Therefore, there exist α, β, $\tau \in \Lambda$ such that $\mathrm{nrd}_{F/K}(\alpha)$ and $\mathrm{nrd}_{F/K}(\beta)$ are coprime and

$$a = \mu\alpha + \mu\beta\tau, \qquad b = \mu\beta.$$

Proof of Lemma 2.3. If b is zero or a unit, the lemma is clear, so we may assume from now on that $\mathrm{nrd}_{F/K}(b)$ is neither zero nor a unit. Let $\mathcal{P}$ be the set of nonzero prime ideals of $\mathbb{Z}_K$ dividing $\mathrm{nrd}_{F/K}(b)$.

First, we want to prove that for any $\mathfrak{p} \in \mathcal{P}$, there exists some $\tau_\mathfrak{p} \in \Lambda$ such that

$$\mathrm{nrd}_{F/K}(a + b\tau_\mathfrak{p}) \notin \mathfrak{p} \quad \text{or} \quad \mathrm{trd}_{F/K}(a + b\tau_\mathfrak{p}) \notin \mathfrak{p}.$$

Obviously, if $\mathrm{nrd}_{F/K}(a) \notin \mathfrak{p}$ or $\mathrm{trd}_{F/K}(a) \notin \mathfrak{p}$, we may take, $\tau_\mathfrak{p} = 0$. Let us assume then that $\mathrm{nrd}_{F/K}(a) \in \mathfrak{p}$ and $\mathrm{trd}_{F/K}(a) \in \mathfrak{p}$. Thanks to Lemma 2.2 (iii), there exists a

[3]Let x, y be two elements of $\mathbb{Z}_K$. We say that x and y are coprime or that x is coprime to y when the ideals $x\mathbb{Z}_K$ and $y\mathbb{Z}_K$ are coprime.

[4]Her proof relied on the following property. Let Λ be a maximal order and let $\mathfrak{N}$ be a maximal ideal with right order Λ. Let $x, y \in \Lambda$ such that $xy \in \mathfrak{N}$. Then x or $y \in \mathfrak{N}$. We have seen in Remark 2.1 that this is incorrect, and even in the totally indefinite case, it is still false. As an example, that we will study later, take $F = \left(\frac{-2,-5}{\mathbb{Q}(\sqrt{-19})}\right)$, $\Lambda = \mathbb{Z}_K \oplus i\mathbb{Z}_K \oplus \frac{1+i+j}{2}\mathbb{Z}_K \oplus \frac{2-i+k}{4}\mathbb{Z}_K$, $\alpha = 1 + i$, and $\mathfrak{N} = \alpha\Lambda$. Then $x = 1 + \frac{2-i+k}{4}$ and $y = \overline{x}$ satisfy $xy = 3 = \mathrm{nrd}_{F/K}(\alpha) \in \mathfrak{N}$. On the one hand, since $h_F = 1$ and $\mathrm{nrd}_{F/K}(\alpha) = 3$, it is easy to see that $\mathfrak{N}$ is maximal. On the other hand, $\mathrm{trd}_{F/K}(\alpha^{-1}x) = \frac{2}{3} \notin \mathbb{Z}_K$ and $\mathrm{trd}_{F/K}(\alpha^{-1}y) = \frac{4}{3} \notin \mathbb{Z}_K$, which implies that neither $x \in \mathfrak{N}$ nor $y \in \mathfrak{N}$.

maximal ideal $\mathfrak{N}$ such that $a \in \mathfrak{N}$ and $\mathfrak{N} \cap \mathbb{Z}_K = \mathfrak{p}$. As $a\Lambda + b\Lambda = \Lambda$, we have $b \notin \mathfrak{N}$, therefore $\mathfrak{N} + b\Lambda = \Lambda$. Consequently, there exist $m \in \mathfrak{N}$ and $\tau_\mathfrak{p} \in \Lambda$ such that

$$1 = m + b\tau_\mathfrak{p}.$$

As a result, $1 - b\tau_\mathfrak{p} \in \mathfrak{N}$. But $1 - b\tau_\mathfrak{p} = 1 - \mathrm{trd}_{F/K}(b\tau_\mathfrak{p}) + \overline{\tau_\mathfrak{p}} \cdot \overline{b}$. If $\mathrm{trd}_{F/K}(b\tau_\mathfrak{p}) \in \mathfrak{p} \subseteq \mathfrak{N}$, then $1 + \overline{\tau_\mathfrak{p}} \cdot \overline{b} \in \mathfrak{N}$. By multiplying on the right by $b \in \Lambda = O_r(\mathfrak{N})$, as $\mathrm{nrd}_{F/K}(b) \in \mathfrak{p}$ we obtain $b \in \mathfrak{N}$, which is impossible. Therefore, $\mathrm{trd}_{F/K}(b\tau_\mathfrak{p}) \notin \mathfrak{p}$, and, as required,

$$\mathrm{trd}_{F/K}(a + b\tau_\mathfrak{p}) \notin \mathfrak{p}.$$

Now, we prove that for any $\mathfrak{p} \in \mathcal{P}$, there exists some $c_\mathfrak{p} \in \Lambda$

$$\mathrm{nrd}_{F/K}(a + bc_\mathfrak{p}) \notin \mathfrak{p}.$$

Fix any $\mathfrak{p} \in \mathcal{P}$. If $\tau_\mathfrak{p}$ is such that $\mathrm{nrd}_{F/K}(a + b\tau_\mathfrak{p}) \notin \mathfrak{p}$, then take $c_\mathfrak{p} = \tau_\mathfrak{p}$. If not, then we have $\mathrm{nrd}_{F/K}(a + b\tau_\mathfrak{p}) \in \mathfrak{p}$ and $\mathrm{trd}_{F/K}(a + b\tau_\mathfrak{p}) \notin \mathfrak{p}$. Let us take any nonzero prime ideal $\mathfrak{q} \neq \mathfrak{p}$ of $\mathbb{Z}_K$. Then $\mathfrak{p}$ and $\mathfrak{q}$ are coprime, so there exist $s \in \mathfrak{p}$ and $t \in \mathfrak{q}$ such that

$$1 = s + t.$$

Besides, as $(a + b\tau_\mathfrak{p})\Lambda + b\Lambda = \Lambda$, there exist λ, $\mu \in \Lambda$ such that

$$1 = (a + b\tau_\mathfrak{p})\lambda + b\mu.$$

Then set $c_\mathfrak{p} = \tau_\mathfrak{p} + \mu t$. We have

$$\begin{aligned} \mathrm{nrd}_{F/K}(a + bc_\mathfrak{p}) = {} & \mathrm{nrd}_{F/K}(a + b\tau_\mathfrak{p}) + \mathrm{nrd}_{F/K}(b\mu t) \\ & + \mathrm{trd}_{F/K}\left((a + b\tau_\mathfrak{p})\overline{b\mu t}\right). \end{aligned} \tag{3}$$

But $\mathrm{nrd}_{F/K}(a + b\tau_\mathfrak{p}) \in \mathfrak{p}$, $\mathrm{nrd}_{F/K}(b\mu t) = \mathrm{nrd}_{F/K}(b)\mathrm{nrd}_{F/K}(\mu t) \in \mathfrak{p}$ and

$$\begin{aligned} \mathrm{trd}_{F/K}\left((a + b\tau_\mathfrak{p})\overline{b\mu t}\right) &= \mathrm{trd}_{F/K}\left((a + b\tau_\mathfrak{p})\overline{1 - (a + b\tau_\mathfrak{p})\lambda}\right) t, \\ &= \mathrm{trd}_{F/K}\left(a + b\tau_\mathfrak{p}\right) t \\ &\quad - \mathrm{trd}_{F/K}\left((a + b\tau_\mathfrak{p}) \cdot \overline{\lambda} \cdot \overline{a + b\tau_\mathfrak{p}}\right) t, \\ &= \left(\mathrm{trd}_{F/K}\left(a + b\tau_\mathfrak{p}\right) - \mathrm{nrd}_{F/K}(a + b\tau_\mathfrak{p})\mathrm{trd}_{F/K}(\lambda)\right) t. \end{aligned}$$

Therefore, (3) shows that $\mathrm{nrd}_{F/K}(a + bc_\mathfrak{p}) = \mathrm{trd}_{F/K}(a + b\tau_\mathfrak{p}) \bmod \mathfrak{p}$, which proves that $\mathrm{nrd}_{F/K}(a + bc_\mathfrak{p}) \notin \mathfrak{p}$, as expected.

Finally, we prove that there exists some $c \in \Lambda$ such that for any $\mathfrak{p} \in \mathcal{P}$, $\mathrm{nrd}_{F/K}(a + bc) \notin \mathfrak{p}$. If $|\mathcal{P}| = 1$, it is clear. If not, let us fix $\mathfrak{p} \in \mathcal{P}$. Then

$$\mathfrak{p} + \prod_{\substack{\mathfrak{q} \in \mathcal{P} \\ \mathfrak{q} \neq \mathfrak{p}}} \mathfrak{q} = \mathbb{Z}_K.$$

So there exist $r_\mathfrak{p} \in \mathfrak{p}$ and $s_\mathfrak{p} \in \prod_{\substack{\mathfrak{q} \in \mathcal{P} \\ \mathfrak{q} \neq \mathfrak{p}}} \mathfrak{q}$ such that

$$r_\mathfrak{p} + s_\mathfrak{p} = 1.$$

Put $c = \sum_{\mathfrak{q} \in \mathcal{P}} s_\mathfrak{q} c_\mathfrak{q}$. Then, for any $\mathfrak{p} \in \mathcal{P}$,

$$c - c_\mathfrak{p} = \sum_{\substack{\mathfrak{q} \in \mathcal{P} \\ \mathfrak{q} \neq \mathfrak{p}}} s_\mathfrak{q} c_\mathfrak{q} - r_\mathfrak{p} c_\mathfrak{p}.$$

As a result, $c - c_\mathfrak{p} \in \mathfrak{p}\Lambda$. Therefore, by Lemma 2.2 (ii),

$$\mathrm{nrd}_{F/K}(a + bc) = \mathrm{nrd}_{F/K}(a + bc_\mathfrak{p}) \bmod \mathfrak{p}.$$

Consequently, for any $\mathfrak{p} \in \mathcal{P}$, $\mathrm{nrd}_{F/K}(a + bc) \notin \mathfrak{p}$.

□

2.2 The Euclidean property

We recall the main properties of Euclidean quaternionic orders seen in [3, §2.3].

Proposition 2.5. *Let Λ be an order of F.*

(i) *Λ is left-Euclidean if and only if Λ is right-Euclidean. Therefore, Λ will be said to be Euclidean if it is left or right-Euclidean. However, it does not mean necessarily that Λ admits a function which is both a left and right-Euclidean stathm.*

(ii) *If Λ is Euclidean, then Λ is maximal.*

(iii) *If Λ is Euclidean, then $h_F = 1$.*

(iv) *If Λ is Euclidean, then every maximal order of F is Euclidean.*

These properties lead to the following definition: A *Euclidean quaternion field* is a quaternion field admitting a Euclidean order, or equivalently such that every maximal order is Euclidean.

2.3 When the stathm is the norm

Let us denote by m_K the local Euclidean minimum map of K (for the norm form) defined by $m_K(x) = \inf_{X \in \mathbb{Z}_K} |N_{K/\mathbb{Q}}(x - X)|$ for $x \in K$. Let $M(K) = \sup_{x \in K} m_K(x)$ be the Euclidean minimum of K. In the same way, let us introduce the notions of local (and global) Euclidean minima of an order Λ of F.

Definition 2.6. For any $\xi \in F$, we set

$$m_\Lambda(\xi) = \inf_{\lambda \in \Lambda} N(\xi - \lambda)$$

and we call it the *local Euclidean minimum* of Λ at ξ. We define the *Euclidean minimum* of Λ by

$$M(\Lambda) = \sup_{\xi \in F} m_\Lambda(\xi).$$

Let us notice that this supremum is a well-defined positive real number and that for every $\xi \in F$ there exists a $\lambda \in \Lambda$ such that $m_\Lambda(\xi) = N(\xi - \lambda)$ (see [4] and [1]).

Proposition 2.7. *The following three statements are equivalent.*

(i) Λ *is left-norm-Euclidean;*

(ii) Λ *is right-norm-Euclidean;*

(iii) For all $\xi \in F$, $m_\Lambda(\xi) < 1$.

Proof. See [3, Proposition 2.13] □

This allows us to speak of a *norm-Euclidean order* without specifying whether it is left norm-Euclidean or right norm-Euclidean. Obviously, with the above notation, if $M(\Lambda) < 1$, then Λ is norm-Euclidean. From Proposition 2.5 (iii), we know that a norm-Euclidean order is necessarily maximal, and, as in the general case, we also have:

Proposition 2.8. *If* F *admits a norm-Euclidean (necessarily maximal) order* Λ*, then every maximal order* Λ' *of* F *is norm-Euclidean. Moreover, we have* $M(\Lambda') = M(\Lambda)$.

Proof. See [3, Proposition 2.14] □

Remark 2.9. Note that the latter equality is true as soon as $t_F = 1$. For a counterexample when $t_F > 1$, see [3, Remark 2.15].

Proposition 2.8 allows us to speak of norm-Euclidean quaternion fields without giving any reference to the maximal order that we consider. A *norm-Euclidean quaternion field* is a quaternion field admitting a norm-Euclidean order, or equivalently such that every maximal order is norm-Euclidean. Moreover if $t_F = 1$, in particular if F

is norm-Euclidean, we can speak without any ambiguity of its *Euclidean minimum*: $M(F) = M(\Lambda)$ for any maximal order Λ of F.

Let us summarize.

- If we want to prove that F is norm-Euclidean, it is sufficient to choose a maximal order Λ of F and to prove that Λ is right norm-Euclidean (or left norm-Euclidean).
- If we want to prove that F is not Euclidean, we have to find a maximal order Λ that is not right-Euclidean (or not left-Euclidean).

3 Euclidean totally indefinite quaternion fields

In this section, F is a totally indefinite quaternion field over K, that is to say no infinite place of K is ramified. This condition has important consequences on the properties of the reduced norm map $\mathrm{nrd}_{F/K}$. The following lemma summarizes them.

Lemma 3.1. *With the above notation, let Λ be a maximal order of F. Then,*

(i) $\mathrm{nrd}_{F/K}(F) = K$;

(ii) $\mathrm{nrd}_{F/K}(\Lambda) = \mathbb{Z}_K$;

(iii) *For any $x \in \Lambda$ and any integral two-sided ideal I of Λ such that $\mathrm{nrd}_{F/K}(x)\mathbb{Z}_K$ and $\mathrm{nrd}_{F/K}(I)$ are coprime, we have*

$$\mathrm{nrd}_{F/K}(x + I) = \mathrm{nrd}_{F/K}(x) + I \cap \mathbb{Z}_K.$$

These properties are usually stated with *Eichler condition*, such a generality is needless for us. Statement (iii) is Eichler's Norm Theorem for the arithmetic progression ([6, Satz 5]), it implies (ii) which is also due to Eichler. In turn, (ii) implies (i), which is a special case of Hasse-Schilling-Maaß Norm Theorem.

These properties have consequences on the class number h_F of F.

Lemma 3.2. *With the above hypotheses, $h_F = h_K$.*

Proof. With the more general Eichler condition, h_F is equal to the order of the ray class group of K modulo the infinite ramified places, which coincides with the class group of K as no infinite place of K is ramified. See [10, Section 35]. □

Remark 3.3. In particular, if F is Euclidean, then $h_F = 1$, thus $h_K = 1$.

Now we can link the Euclidean properties of the number field K and of the quaternion field F.

Theorem 3.4. *Let F be a totally indefinite quaternion field over a number field K. Then the following statements hold.*

(i) *If K is Euclidean, then F is Euclidean;*

(ii) *If K is norm-Euclidean, then F is norm-Euclidean;*

(iii) *Suppose that $h_K = 1$. Then for any maximal order Λ of F, we have $M(\Lambda) \leq M(K)$.*

Proof. We will start by proving (i) and (ii). Let us assume that K is Euclidean, which implies $h_F = h_K = 1$. Let $\varphi : \mathbb{Z}_K \longrightarrow W$ be a Euclidean stathm for some well-ordered set W. Set Λ to be a maximal order of F. We put $\Phi = \varphi \circ \mathrm{nrd}_{F/K} : \Lambda \longrightarrow W$ and we will prove that Φ is a right-Euclidean stathm.

Let $\alpha, \beta \in \Lambda$. Then, using Lemma 2.3 and Remark 2.4, there exists $(\mu, \alpha', \beta', \tau) \in \Lambda^4$ such that $\beta = \mu\beta'$, $\alpha = \mu\alpha' + \mu\beta'\tau$, and $\mathrm{nrd}_{F/K}(\alpha')$ and $\mathrm{nrd}_{F/K}(\beta')$ are coprime. Since φ is a Euclidean stathm, we can divide $\mathrm{nrd}_{F/K}(\mu)\mathrm{nrd}_{F/K}(\alpha')$ by $\mathrm{nrd}_{F/K}(\mu)\mathrm{nrd}_{F/K}(\beta') = \mathrm{nrd}_{F/K}(\beta)$ and there exists a $c \in \mathbb{Z}_K$ such that

$$\varphi\left(\mathrm{nrd}_{F/K}(\mu)\mathrm{nrd}_{F/K}(\alpha') - \mathrm{nrd}_{F/K}(\mu)\mathrm{nrd}_{F/K}(\beta')c\right) < \varphi(\mathrm{nrd}_{F/K}(\beta)). \tag{4}$$

Now, notice that $\mathrm{nrd}_{F/K}(\alpha') - \mathrm{nrd}_{F/K}(\beta')c \in \mathrm{nrd}_{F/K}(\alpha') + \mathrm{nrd}_{F/K}(\beta')\mathbb{Z}_K$. We may then apply Lemma 3.1 (iii) with $I = \mathrm{nrd}_{F/K}(\beta')\Lambda$ and $x = \alpha'$. We obtain $\mathrm{nrd}_{F/K}(\alpha') + \mathrm{nrd}_{F/K}(\beta')\mathbb{Z}_K = \mathrm{nrd}_{F/K}\left(\alpha' + \mathrm{nrd}_{F/K}(\beta')\Lambda\right) \subseteq \mathrm{nrd}_{F/K}(\alpha' + \beta'\Lambda)$. This allows us to write $\mathrm{nrd}_{F/K}(\alpha') - \mathrm{nrd}_{F/K}(\beta')c = \mathrm{nrd}_{F/K}(\alpha' - \beta'\gamma)$ for a $\gamma \in \Lambda$. Consequently,

$$\mathrm{nrd}_{F/K}(\mu)\mathrm{nrd}_{F/K}(\alpha') - \mathrm{nrd}_{F/K}(\mu)\mathrm{nrd}_{F/K}(\beta')c = \mathrm{nrd}_{F/K}(\mu)\mathrm{nrd}_{F/K}(\alpha' - \beta'\gamma),$$

and (4) can be rewritten as

$$\varphi(\mathrm{nrd}_{F/K}(\alpha - \beta(\tau + \gamma))) < \varphi(\mathrm{nrd}_{F/K}(\beta)),$$

which completes the proof of (i).

If we assume K to be norm-Euclidean, then we can take $\varphi = |N_{K/\mathbb{Q}}| : \mathbb{Z}_K \longrightarrow \mathbb{Z}_{\geq 0}$. We proved above that $\Phi = N$ is a right-Euclidean stathm for Λ, that is to say that F is norm-Euclidean. That proves (ii).

Now, we will prove (iii). Take $\xi \in F$. Since $h_K = 1$ we also have $h_F = 1$ by Lemma 3.2, and thanks to Lemma 2.3 and Remark 2.4, ξ can be written as $\xi = \beta^{-1}\alpha + \tau$ for some $\alpha, \beta, \tau \in \Lambda$ such that $\mathrm{nrd}_{F/K}(\alpha)$ and $\mathrm{nrd}_{F/K}(\beta)$ are coprime. Then, we can take a $c \in \mathbb{Z}_K$ such that

$$\left|N_{K/\mathbb{Q}}\left(\mathrm{nrd}_{F/K}(\beta^{-1}\alpha) - c\right)\right| = m_K\left(\mathrm{nrd}_{F/K}(\beta^{-1}\alpha)\right). \tag{5}$$

As before, Lemma 3.1 (iii) proves that

$$\begin{aligned}\mathrm{nrd}_{F/K}(\alpha)+\mathrm{nrd}_{F/K}(\beta)\mathbb{Z}_K &= \mathrm{nrd}_{F/K}\left(\alpha+\mathrm{nrd}_{F/K}(\beta)\Lambda\right)\\ &\subseteq \mathrm{nrd}_{F/K}\left(\alpha+\beta\tau+\beta\Lambda\right).\end{aligned}$$

We deduce from it that there exists a $\gamma\in\Lambda$ such that

$$\mathrm{nrd}_{F/K}(\alpha)-\mathrm{nrd}_{F/K}(\beta)c=\mathrm{nrd}_{F/K}\left(\alpha+\beta\tau-\beta\gamma\right).$$

Dividing by $\mathrm{nrd}_{F/K}(\beta)$ and using (5), we find

$$\left|N_{K/\mathbb{Q}}(\mathrm{nrd}_{F/K}(\xi-\gamma))\right|=m_K\left(\mathrm{nrd}_{F/K}(\beta^{-1}\alpha)\right).$$

Therefore, we have $m_\Lambda(\xi)\leq m_K\left(\mathrm{nrd}_{F/K}(\beta^{-1}\alpha)\right)\leq M(K)$, from which we easily deduce (iii). □

Now, we can complete the list of Euclidean and norm-Euclidean quaternion fields over $\mathbb{Q}$.

Corollary 3.5. *Let F be a quaternion field over $\mathbb{Q}$. Then F is Euclidean if and only if F is norm-Euclidean, which happens exactly when F is indefinite or*

$$F\in\left\{\left(\frac{-1,-1}{\mathbb{Q}}\right),\left(\frac{-1,-3}{\mathbb{Q}}\right),\left(\frac{-2,-5}{\mathbb{Q}}\right)\right\}.$$

Proof. The case where F is definite over $\mathbb{Q}$ was treated in [3, Section 4]. If F is indefinite over $\mathbb{Q}$, then F is norm-Euclidean thanks to Theorem 3.4 (ii). □

Remark 3.6. The Euclidean and the norm-Euclidean properties are equivalent in this setting. This is analogous to the cases of imaginary quadratic number fields and totally definite quaternion fields over quadratic number fields (see [3]).

So far, all examples of Euclidean quaternion fields were in fact norm-Euclidean. As there exist Euclidean number fields which are not norm-Euclidean, we can use Theorem 3.4 (i) to find quaternion fields which are Euclidean, but *not necessarily* norm-Euclidean. To exhibit examples which are actually *not* norm-Euclidean, we will need the following lemma.

Lemma 3.7. *Let F a totally indefinite quaternion field over a number field K with $h_K=1$. Let $\mathfrak{p}_i$, $1\leq i\leq s$ be some distinct finite places of K ramified in F and $t\in\mathbb{Z}_K$ such that $t\mathbb{Z}_K=\mathfrak{p}_1\cdots\mathfrak{p}_s$ (we have $h_K=1$). Then for any $v\in\mathbb{Z}_K$ coprime to t, there exists $\xi\in F$ such that $m_\Lambda(\xi)\geq m_K(v/t)$.*

Proof. First, by Lemma 3.1 (ii), there exists an $a \in \Lambda$ such that $\mathrm{nrd}_{F/K}(a) = v$. For every i, let us denote by $\mathfrak{P}_i$ the unique prime two-sided ideal of Λ lying above $\mathfrak{p}_i$. These ideals satisfy: $\mathfrak{p}_i\Lambda = \mathfrak{P}_i^2$, $\mathfrak{P}_i \cap \mathbb{Z}_K = \mathfrak{p}_i$ and $\mathfrak{P}_i\mathfrak{P}_j = \mathfrak{P}_j\mathfrak{P}_i$ for every i, j (see [10, Section 22]). Moreover $\mathrm{nrd}_{F/K}(\mathfrak{P}_i) = \mathfrak{p}_i$. Since the $\mathfrak{P}_i$ commute, we have $\mathfrak{P}_1 \cdots \mathfrak{P}_s \subseteq \mathfrak{P}_i$ for every i. This implies $\mathfrak{P}_1 \cdots \mathfrak{P}_s \cap \mathbb{Z}_K \subseteq \mathfrak{P}_i \cap \mathbb{Z}_K = \mathfrak{p}_i$ for every i so that

$$\mathfrak{P}_1 \cdots \mathfrak{P}_s \cap \mathbb{Z}_K \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_s.$$

Let us notice that $\mathrm{nrd}_{F/K}(a)\mathbb{Z}_K = v\mathbb{Z}_K$ and $\mathrm{nrd}_{F/K}(\mathfrak{P}_1 \cdots \mathfrak{P}_s) = \mathfrak{p}_1 \cdots \mathfrak{p}_s = t\mathbb{Z}_K$ are coprime. Applying Lemma 3.1 (iii) to $x = a$ and $I = \mathfrak{P}_1 \cdots \mathfrak{P}_s$, we obtain

$$\begin{aligned} \mathrm{nrd}_{F/K}(a + \mathfrak{P}_1 \cdots \mathfrak{P}_s) &= \mathrm{nrd}_{F/K}(a) + \mathfrak{P}_1 \cdots \mathfrak{P}_s \cap \mathbb{Z}_K \\ &\subseteq \mathrm{nrd}_{F/K}(a) + \mathfrak{p}_1 \cdots \mathfrak{p}_s. \end{aligned} \tag{6}$$

Since $h_F = 1$, there exists a $b \in \Lambda$ such that $\mathfrak{P}_1 \cdots \mathfrak{P}_s = b\Lambda$. Let us put $\xi = b^{-1}a \in F$. Then, there exists a $\lambda \in \Lambda$ such that

$$\begin{aligned} m_\Lambda(\xi) &= \frac{N(a - b\lambda)}{N(b)} \\ &= \frac{|N_{K/\mathbb{Q}}(\mathrm{nrd}_{F/K}(a - b\lambda))|}{N(b)}. \end{aligned}$$

As $b\lambda \in \mathfrak{P}_1 \cdots \mathfrak{P}_s$, (6) shows that there exists a $y \in \mathfrak{p}_1 \cdots \mathfrak{p}_s = t\mathbb{Z}_K$ such that

$$\mathrm{nrd}_{F/K}(a - b\lambda) = \mathrm{nrd}_{F/K}(a) + y.$$

Hence there exists a $z \in \mathbb{Z}_K$ such that

$$m_\Lambda(\xi) = \frac{|N_{K/\mathbb{Q}}(\mathrm{nrd}_{F/K}(a) + tz)|}{N(b)}.$$

But $\mathrm{nrd}_{F/K}(b) \in \mathbb{Z}_K$ and $\mathrm{nrd}_{F/K}(b)\mathbb{Z}_K = \mathrm{nrd}_{F/K}(\mathfrak{P}_1 \cdots \mathfrak{P}_s) = \mathfrak{p}_1 \cdots \mathfrak{p}_s = t\mathbb{Z}_K$ so that we have $\mathrm{nrd}_{F/K}(b) = \varepsilon t$ where $\varepsilon \in \mathbb{Z}_K^\times$. From this we deduce

$$\begin{aligned} m_\Lambda(\xi) &= \frac{|N_{K/\mathbb{Q}}(\mathrm{nrd}_{F/K}(a) + tz)|}{|N_{K/\mathbb{Q}}(\varepsilon t)|} \\ &= \frac{|N_{K/\mathbb{Q}}(v + tz)|}{|N_{K/\mathbb{Q}}(t)|} \\ &= \left|N_{K/\mathbb{Q}}\left(\frac{v}{t} + z\right)\right| \\ &\geq m_K\left(\frac{v}{t}\right). \end{aligned}$$

□

Proposition 3.8. *Let K be the real quadratic field of discriminant 53. We set $x \in K$ such that $x^2 - x - 13 = 0$. We put $t = x + 2$ and $\mathfrak{p} = t\mathbb{Z}_K$. Let F be any totally indefinite quaternion field over K in which $\mathfrak{p}$ is ramified. For instance, we can take $F = \left(\frac{-1, 7}{K}\right)$. Then F is Euclidean, but not norm-Euclidean.*

Proof. Take any F satisfying the conditions of the proposition. As F is totally indefinite, $h_F = h_K = 1$. Harper proved that K is Euclidean (without assuming GRH, see [7]). Consequently, by Theorem 3.4 (i), F is Euclidean.

Furthermore, let us define $v = 2x + 7$, which is coprime to t. Then, by Lemma 3.7, there exists some $\xi \in F$ such that $m_\Lambda(\xi) \geq m_K\left(\frac{v}{t}\right)$. But we chose v and t such that $m_K\left(\frac{v}{t}\right) = M(K) = \frac{9}{7}$. Therefore, $m_\Lambda(\xi) \geq 1$, which proves that F is not norm-Euclidean. □

4 Quaternion fields over imaginary quadratic number fields

The section will be devoted to the proof of the following statement.

Theorem 4.1. *Let $K = \mathbb{Q}(\sqrt{-d})$ (where d is a squarefree positive integer) be an imaginary quadratic number field. Let F be a quaternion field over K. Then F is norm-Euclidean if and only if $d \in \{1, 2, 3, 7, 11\}$ or $F = \left(\frac{-2, -5}{\mathbb{Q}(\sqrt{-19})}\right)$.*

In this section, K is an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-d})$, where $d > 0$ is a squarefree integer, and F is a quaternion field over K. Let us remark that no infinite place of K ramifies in F, so that F is totally indefinite. Suppose that F is norm-Euclidean. Since F is totally indefinite, by Lemma 3.2, we have $h_K = h_F = 1$. This implies that $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. In Subsection 3.1 we will prove that F is norm-Euclidean for $d = 1, 2, 3, 7, 11$ and not norm-Euclidean for $d > 19$. Then, Subsection 3.2 will be devoted to the remaining case $d = 19$, and we will prove that under this hypothesis the only norm-Euclidean quaternion field is $\left(\frac{-2, -5}{\mathbb{Q}(\sqrt{-19})}\right)$, thus proving Theorem 4.1.

4.1 First steps, the case $d \neq 19$

First, we can deal with the 5 first values of d.

Proposition 4.2. *If $d = 1, 2, 3, 7$ or 11, then F is norm-Euclidean.*

Proof. It is a classical fact that $d = 1, 2, 3, 7$ and 11 are the only values of d for which K is norm-Euclidean. Then, thanks to Theorem 3.4 (ii), we conclude that F is norm-Euclidean. □

Now, in view of proving that F cannot be norm-Euclidean for $d > 19$ we have to establish some preliminary results. In particular, in order to apply Lemma 3.7, we look for convenient points $x \in K$ such that $m_K(x) \geq 1$.

Lemma 4.3. *Suppose that* $d \in \{19, 43, 67, 163\}$. *If* $t \in \mathbb{Z}_K$ *satisfies*

(i) *either* $t \in \mathbb{Z}$ *and* $|t| \geq \dfrac{\sqrt{d}}{\sqrt{d}-4}$

(ii) *or* $t \notin \mathbb{Z}$ *and* $|t| \geq \dfrac{2}{\sqrt{d}-4}$

then, there exists some $v \in \mathbb{Z}_K$ *such that* $m_K(v/t) \geq 1$.

Proof. In all cases, we have $d \equiv 3 \bmod 4$ and $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\omega$ where $\omega = \frac{1+\sqrt{-d}}{2}$. Let us put

$$\mathcal{B} = \left\{ x \in K;\ 1 \leq \mathrm{Im}(x) \leq \frac{\sqrt{d}}{2} - 1 \right\}.$$

It is easy to see that if $x \in \mathcal{B}$ then $m_K(x) \geq 1$. Thus, it is sufficient to find $v \in \mathbb{Z}_K$ such that $v/t \in \mathcal{B}$. Let us write $t = t_1 + t_2\omega$ where $t_1,\ t_2 \in \mathbb{Z}$.
Case (i)*:* $t \in \mathbb{Z}$ $(t_2 = 0)$. Let us search for such a v with $v = k\omega$ and $k \in \mathbb{Z}$ with the same sign as t. Since $\mathrm{Im}\left(\dfrac{v}{t}\right) = \dfrac{k\sqrt{d}}{2t}$, we have

$$\frac{v}{t} \in \mathcal{B} \Longleftrightarrow \frac{2|t|}{\sqrt{d}} \leq |k| \leq \frac{(\sqrt{d}-2)|t|}{\sqrt{d}}.$$

But condition (i) implies that the difference between the right-hand side and the left-hand side of this double inequality is at least 1, so that we can find such a k.
Case (ii)*:* $t \notin \mathbb{Z}$ $(t_2 \neq 0)$. Here, let us search for v in $\mathbb{Z}$, whose sign is opposite to the sign of t_2. Since $\mathrm{Im}\left(\dfrac{v}{t}\right) = -\dfrac{vt_2\sqrt{d}}{2|t|^2}$, we have

$$\frac{v}{t} \in \mathcal{B} \Longleftrightarrow \frac{2|t|^2}{|t_2|\sqrt{d}} \leq |v| \leq \frac{|t|^2(\sqrt{d}-2)}{|t_2|\sqrt{d}}.$$

As above, such a v exists if $\dfrac{|t|^2(\sqrt{d}-4)}{|t_2|\sqrt{d}} \geq 1$. But since $\dfrac{|t|}{|t_2|} \geq \dfrac{\sqrt{d}}{2}$ it is sufficient to have $\dfrac{|t|(\sqrt{d}-4)}{2} \geq 1$ which is implied by condition (ii). □

Proposition 4.4. *If* $d \in \{43, 67, 163\}$, *then* F *is not norm-Euclidean.*

Proof. In these three cases, $K = \mathbb{Q}(\sqrt{-d})$ has class number 1. Recall also that, since F is totally indefinite, the set $\mathcal{S}$ of finite primes of K that ramify in F is non-empty and has even cardinality. Let $\mathfrak{p}$ be such a prime. Since $h_K = 1$, there exists a $t \in \mathbb{Z}_K$ with $\mathfrak{p} = t\mathbb{Z}_K$. Moreover $|t| > 1$ because $\mathfrak{p}$ is prime.

For $d = 67$ and 163 we have $\dfrac{\sqrt{d}}{\sqrt{d}-4} < 2$, $\dfrac{2}{\sqrt{d}-4} < 1$ and necessarily t satisfies hypotheses of Lemma 4.3. This implies that there exists a $v \in \mathbb{Z}_K$ such that $m_K(v/t) \geq 1$. But v and t are coprime: if not, $t\mathbb{Z}_K$ being a prime ideal, we would have $v/t \in \mathbb{Z}_K$ and $m_K(v/t) = 0$, which is absurd. Hence, we can apply Lemma 3.7 with $s = 1$ and there exists a $\xi \in F$ such that $m_\Lambda(\xi) \geq m_K(v/t) \geq 1$. Consequently, F is not norm-Euclidean.

For $d = 43$ we have $\dfrac{\sqrt{d}}{\sqrt{d}-4} < 3$ and $\dfrac{2}{\sqrt{d}-4} < 1$. The same argument is possible if $t \notin \mathbb{Z}$ or $t \in \mathbb{Z}$ with $|t| \geq 3$. It remains to study the case where $t = \pm 2$. But, as the cardinality of $\mathcal{S}$ is a positive even integer, there exists another finite prime that ramifies in F, say $\mathfrak{p}' = t'\mathbb{Z}_K$. If $t' \notin \mathbb{Z}$, we are done. If $t' \in \mathbb{Z}$, necessarily $|t'| \geq 3$ because $\mathfrak{p}' \neq \mathfrak{p}$. We can apply again Lemma 4.3 with t' and the conclusion follows. □

Summarizing results of Proposition 4.2 and Proposition 4.4, we obtain

Theorem 4.5. *For $d \neq 19$, F is norm-Euclidean if and only if*

$$d \in \{1, 2, 3, 7, 11\}.$$

4.2 The case $d = 19$

It remains to study the case $d = 19$. We are first going to prove that there is only one quaternion field over $\mathbb{Q}(\sqrt{-19})$ that might be norm-Euclidean.

Proposition 4.6. *If F is a norm-Euclidean quaternion field over $\mathbb{Q}(\sqrt{-19})$, then necessarily $F = \left(\dfrac{-2,-5}{\mathbb{Q}(\sqrt{-19})}\right)$.*

Proof. For $d = 19$ we have $\dfrac{\sqrt{d}}{\sqrt{d}-4} < 13$ and $\dfrac{2}{\sqrt{d}-4} < \sqrt{32}$. The same argument as above shows that if $\mathfrak{p} = t\mathbb{Z}_K$ is a finite prime of $\mathbb{Z}_K$ that ramifies in F, then we have $|t|^2 \leq 31$ if $t \notin \mathbb{Z}$ and $|t| \leq 12$ otherwise. This leads to the following list of candidates: the primes $\mathfrak{p}_2 = 2\mathbb{Z}_K$, $\mathfrak{p}_3 = 3\mathbb{Z}_K$, $\mathfrak{p}_5 = \omega\mathbb{Z}_K$, $\overline{\mathfrak{p}_5}$, $\mathfrak{p}_7 = (1+\omega)\mathbb{Z}_K$, $\overline{\mathfrak{p}_7}$, $\mathfrak{p}_{11} = (2+\omega)\mathbb{Z}_K$, $\overline{\mathfrak{p}_{11}}$, $\mathfrak{p}_{17} = (3+\omega)\mathbb{Z}_K$, $\overline{\mathfrak{p}_{17}}$, $\mathfrak{p}_{19} = (-1+2\omega)\mathbb{Z}_K$, $\overline{\mathfrak{p}_{19}}$, $\mathfrak{p}_{23} = (1+2\omega)\mathbb{Z}_K$, $\overline{\mathfrak{p}_{23}}$. Here $\mathfrak{p}_m$ is the prime above m when m is inert, otherwise the two primes above m are $\mathfrak{p}_m$ and $\overline{\mathfrak{p}_m}$ (its conjugate). Now, it is easy to compute some appropriate local Euclidean minima in K. We obtain

$$m_K\left(\frac{\omega}{2}\right) = \frac{5}{4},\ m_K\left(\frac{3}{1+\omega}\right) = m_K\left(\frac{3}{1+\overline{\omega}}\right) = 1,$$
$$m_K\left(\frac{5}{2+\omega}\right) = m_K\left(\frac{5}{2+\overline{\omega}}\right) = 1,\ m_K\left(\frac{7}{3+\omega}\right) = m_K\left(\frac{7}{3+\overline{\omega}}\right) = 1,$$
$$m_K\left(\frac{5}{2\omega-1}\right) = m_K\left(\frac{7}{2\overline{\omega}-1}\right) = \frac{25}{19},$$
$$m_K\left(\frac{5}{2\omega+1}\right) = m_K\left(\frac{5}{2\overline{\omega}+1}\right) = \frac{25}{23}.$$

In all these cases, Lemma 3.7 (with $s = 1$) can be applied and we obtain that only $\mathfrak{p}_3$, $\mathfrak{p}_5$ and $\overline{\mathfrak{p}_5}$ can be ramified in F. Moreover we have

$$m_K\left(\frac{7}{3\omega}\right) = m_K\left(\frac{7}{3\overline{\omega}}\right) = \frac{49}{45}.$$

Again Lemma 3.7 (with $s = 2$) shows that neither $\mathfrak{p}_3$ and $\mathfrak{p}_5$, nor $\mathfrak{p}_3$ and $\overline{\mathfrak{p}_5}$ can be ramified simultaneously. Since the number of finite ramified primes is a positive even integer, we have a unique possibility: $\mathfrak{p}_5$ and $\overline{\mathfrak{p}_5}$ are the only primes of K that ramify in F. This leads (up to isomorphism) to

$$F = \left(\frac{-2,-5}{\mathbb{Q}(\sqrt{-19})}\right).$$

□

Remark 4.7. We have $m_K\left(\frac{1+2\omega}{\omega\overline{\omega}}\right) = \frac{23}{25}$ and the primes $\mathfrak{p}_5$ and $\overline{\mathfrak{p}_5}$ are ramified. Therefore, Lemma 3.7 gives us the following bound:

$$M(\Lambda) \geq \frac{23}{25}. \tag{7}$$

Now let us focus on $F = \left(\frac{-2,-5}{\mathbb{Q}(\sqrt{-19})}\right)$. As a maximal order of F, we can take[5]

$$\Lambda = \mathbb{Z}_K \oplus i\mathbb{Z}_K \oplus \frac{1+i+j}{2}\mathbb{Z}_K \oplus \frac{2-i+k}{4}\mathbb{Z}_K.$$

We are going to prove that F is norm-Euclidean. Our approach will be algorithmic, following some ideas used in [2], [8] and [3] for the computation of the Euclidean minimum. Let us work in a more general context. Let $d > 1$ be a squarefree integer and $F = \left(\frac{a,b}{K}\right)$ be a totally indefinite quaternion field over $K = \mathbb{Q}(\sqrt{-d})$, where a, b

[5]We do not prove this because it is easy to check that Λ is an order whose discriminant is equal to -5^2. It can also be checked using Magma ([9]).

are supposed to belong to $\mathbb{Q}$, for simplicity. Let Λ be a maximal order of F. Suppose that we have a description of Λ:

$$\Lambda = \bigoplus_{l=1}^{4} (a_{l,1} + a_{l,2}i + a_{l,3}j + a_{l,4}k)\mathbb{Z}_K,$$

where, for simplicity, we suppose that $a_{l,m} \in \mathbb{Q}$ for $1 \leq l,\, m \leq 4$. Then F can be written

$$\begin{aligned} F &= \bigoplus_{l=1}^{4} (a_{l,1} + a_{l,2}i + a_{l,3}j + a_{l,4}k)K \\ &= \Lambda + \Delta, \end{aligned}$$

where

$$\Delta = \bigoplus_{l=1}^{4} (a_{l,1} + a_{l,2}i + a_{l,3}j + a_{l,4}k)D,$$

and where D is a fundamental domain of K. Take for instance $D = \{x + y\theta;\ x, y \in J\}$, where $J = [0,\, 1) \cap \mathbb{Q}$ and

$$\theta = \begin{cases} \frac{1+\sqrt{-d}}{2} & \text{if } d \equiv 3 \bmod 4, \\ \sqrt{-d} & \text{otherwise.} \end{cases}$$

Now, since m_Λ is Λ-periodic, to prove that F is norm-Euclidean, it is sufficient to establish that for every $\xi \in \Delta$ there exists a $\lambda \in \Lambda$ such that $N(\xi - \lambda) < 1$. The sets Λ and Δ can be rewritten as

$$\Lambda = \left\{ \sum_{l=1}^{4} a_{l,1}z_l + i\sum_{l=1}^{4} a_{l,2}z_l + j\sum_{l=1}^{4} a_{l,3}z_l + k\sum_{l=1}^{4} a_{l,4}z_l;\ x_l,\, y_l \in \mathbb{Z} \right\},$$

$$\Delta = \left\{ \sum_{l=1}^{4} a_{l,1}z_l + i\sum_{l=1}^{4} a_{l,2}z_l + j\sum_{l=1}^{4} a_{l,3}z_l + k\sum_{l=1}^{4} a_{l,4}z_l;\ x_l,\, y_l \in J \right\},$$

where $z_l = x_l + y_l\theta$. Clearly, Λ and Δ are respectively isomorphic to $\mathbb{Z}^8$ and J^8, and we embed both sets in $\mathbb{R}^8$ in the following way. To $\xi = \alpha + \beta i + \gamma j + \delta k \in F$, where $\alpha, \beta, \gamma, \delta \in K$ we associate the column vector

$$\big(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha), \mathrm{Re}(\beta), \mathrm{Im}(\beta), \mathrm{Re}(\gamma), \mathrm{Im}(\gamma), \mathrm{Re}(\delta), \mathrm{Im}(\delta)\big)^{\mathsf{T}}.$$

In other words, we consider the matrix $M \in M_{8\times 8}(\mathbb{R})$ defined by

$$M = \begin{pmatrix} a_{1,1} & a_{1,1}\eta & a_{2,1} & a_{2,1}\eta & a_{3,1} & a_{3,1}\eta & a_{4,1} & a_{4,1}\eta \\ 0 & a_{1,1}\mu & 0 & a_{2,1}\mu & 0 & a_{3,1}\mu & 0 & a_{4,1}\mu \\ a_{1,2} & a_{1,2}\eta & a_{2,2} & a_{2,2}\eta & a_{3,2} & a_{3,2}\eta & a_{4,2} & a_{4,2}\eta \\ 0 & a_{1,2}\mu & 0 & a_{2,2}\mu & 0 & a_{3,2}\mu & 0 & a_{4,2}\mu \\ a_{1,3} & a_{1,3}\eta & a_{2,3} & a_{2,3}\eta & a_{3,3} & a_{3,3}\eta & a_{4,3} & a_{4,3}\eta \\ 0 & a_{1,3}\mu & 0 & a_{2,3}\mu & 0 & a_{3,3}\mu & 0 & a_{4,3}\mu \\ a_{1,4} & a_{1,4}\eta & a_{2,4} & a_{2,4}\eta & a_{3,4} & a_{3,4}\eta & a_{4,4} & a_{4,4}\eta \\ 0 & a_{1,4}\mu & 0 & a_{2,4}\mu & 0 & a_{3,4}\mu & 0 & a_{4,4}\mu \end{pmatrix},$$

where $\eta = \mathrm{Re}(\theta)$ and $\mu = \mathrm{Im}(\theta)$, and we see Λ and Δ respectively as $M \cdot \mathbb{Z}^8$ and $M \cdot J^8$. Now, we consider a cutting-covering of $\overline{\Delta} = M \cdot [0,\, 1]^8$ using parallelotopes whose faces are orthogonal to the canonical axes of $\mathbb{R}^8$. These parallelotopes $\mathcal{P}$ are of the form

$$\mathcal{P} = \{(u_i)_{1 \leq i \leq 8} \in \mathbb{R}^8;\, |u_i - C_i| \leq h_i\},$$

where $C = (c_i)_{1 \leq i \leq 8}$ is the center of the parallelotope and $0 < h_i$ for every i. In order to prove that F is norm-Euclidean, it is sufficient to prove that for every $\mathcal{P}$ of our cutting-covering of $\overline{\Delta}$ there exists a $\lambda \in \Lambda$ such that

$$\text{for every } u \in \mathcal{P},\ N(u - \lambda) < 1. \tag{8}$$

In this case, we will say that $\mathcal{P}$ is absorbed by λ. But thanks to our identification N can be rewritten

$$\begin{aligned} N(t) &= \left|(t_1 + t_2 I)^2 - a(t_3 + t_4 I)^2 - b(t_5 + t_6 I)^2 + ab(t_7 + t_8 I)^2\right|^2 \\ &= f(t)^2 + 4g(t)^2, \end{aligned}$$

where I is a complex square root of -1 and

$$\left\{ \begin{array}{rcl} f(t) &=& t_1^2 - t_2^2 - at_3^2 + at_4^2 - bt_5^2 + bt_6^2 + abt_7^2 - abt_8^2, \\ g(t) &=& t_1 t_2 - at_3 t_4 - bt_5 t_6 + abt_7 t_8. \end{array} \right.$$

Therefore, to ensure that (8) is satisfied, it is enough to establish that

$$A(\mathcal{P},\, \lambda) + 4B(\mathcal{P},\, \lambda) < 1, \tag{9}$$

where

$$A(\mathcal{P},\, \lambda) = \sup_{t \in \mathcal{P} - \lambda} f(t)^2 \quad \text{and} \quad B(\mathcal{P},\, \lambda) = \sup_{t \in \mathcal{P} - \lambda} g(t)^2.$$

Let us remark that, if $y_i = C_i - \lambda_i$, for every $t \in \mathcal{P} - \lambda$, we have $t_i \in [y_i - h_i, y_i + h_i]$, from which we deduce

$$\left\{ \begin{array}{rcccll} 0 &\leq& t_i^2 &\leq& y_i^2 + 2|y_i|h_i + h_i^2 & \text{if } |y_i| \leq h_i \\ y_i^2 - 2|y_i|h_i + h_i^2 &\leq& t_i^2 &\leq& y_i^2 + 2|y_i|h_i + h_i^2 & \text{if } |y_i| \geq h_i \end{array} \right.$$

and

$$y_i y_j - |y_i|h_j - |y_j|h_i - h_i h_j \leq t_i t_j \leq y_i y_j + |y_i|h_j + |y_j|h_i + h_i h_j.$$

If we take into account the signs of a and b, these inequalities give us explicit bounds for $f(t)$ and $g(t)$ when $t \in \mathcal{P} - \lambda$, say $\alpha \leq f(t) \leq \beta$ and $\gamma \leq g(t) \leq \delta$, from which we deduce that (9) will be satisfied if

$$\max\{\alpha^2, \beta^2\} + 4\max\{\gamma^2, \delta^2\} < 1. \tag{10}$$

Now, it is sufficient to prove that every $\mathcal{P}$ of our cutting-covering satisfies (10) for some λ belonging to a finite set $\mathcal{S}$ of precomputed elements of Λ. Of course, things are not so simple: in general, if we begin with a reasonable cutting-covering, some parallelotopes are not absorbed. In this case, we cut them into 2^8 smaller parallelotopes and we continue. The algorithm is roughly as follows.

1. Define a set $\mathcal{S}$ of elements of Λ.
2. Define a covering of $\overline{\Delta}$ by parallelotopes as described above. Denote by T the set of these parallelotopes.
3. For any $\mathcal{P} \in T$, search for a λ in S that absorbs $\mathcal{P}$, replacing 1 by a constant $k < 1$ in (10) to control rounding errors. If such a λ exists, remove $\mathcal{P}$ from T.
4. If $T = \emptyset$, we are done and the algorithm stops.
5. If not, cut every $\mathcal{P} \in T$ into 2^8 smaller parallelotopes and replace T with the set of these smaller parallelotopes. Then go to step (3).

In the case of F we have $K = \mathbb{Q}(\sqrt{-19})$, $\theta = \frac{1+\sqrt{-19}}{2}$ and as a maximal order for F we take $\Lambda = \mathbb{Z}_K \oplus i\mathbb{Z}_K \oplus \frac{1+i+j}{2}\mathbb{Z}_K \oplus \frac{2-i+k}{4}\mathbb{Z}_K$ so that our matrix M is

$$M = \begin{pmatrix} 1 & \frac{1}{2} & 0 & 0 & \frac{1}{2} & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & \frac{\sqrt{19}}{2} & 0 & 0 & 0 & \frac{\sqrt{19}}{4} & 0 & \frac{\sqrt{19}}{4} \\ 0 & 0 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{4} & -\frac{1}{4} & -\frac{1}{8} \\ 0 & 0 & 0 & \frac{\sqrt{19}}{2} & 0 & \frac{\sqrt{19}}{4} & 0 & -\frac{\sqrt{19}}{8} \\ 0 & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{19}}{4} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{4} & \frac{1}{8} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{19}}{8} \end{pmatrix}.$$

The algorithm ran with the following parameters: the set $\mathcal{S}$ was defined by

$$\mathcal{S} = \{M \cdot X;\ X_i \in \mathbb{Z} \cap [-2, 3] \text{ for every } i\},$$

we used a covering of $\overline{\Delta}$ by parallelotopes satisfying, with the above notation,

$$h_i = \frac{\max\{x_i;\ x \in \overline{\Delta}\} - \min\{x_i;\ x \in \overline{\Delta}\}}{120}$$

for every i, and the constant k was equal to 0.921. After 3 loops, all parallelotopes were absorbed at one step or another and we obtained:

Proposition 4.8. *The quaternion field F is norm-Euclidean.*

Combining Theorem 4.5, Proposition 4.6 and Proposition 4.8 completes the proof of Theorem 4.1.

Remark 4.9. If we take $k = 0.92$, the algorithm does not succeed. There are many problematic parallelotopes and after several loops, their number increases dramatically. Since we know that $M(\Lambda) \geq \frac{23}{25}$ it is reasonable to conjecture that we have an equality.

Remark 4.10. This gives a negative answer to the question asked by Eichler. Here $K = \mathbb{Q}(\sqrt{-19})$ is not norm-Euclidean and even not Euclidean for any stathm, but $F = \left(\frac{-2,-5}{K}\right)$ is norm-Euclidean. Let us note that Eichler's definition of the Euclidean property for K was slightly different than the standard one that we use. Anyway, in our context, both definitions are equivalent.

Acknowledgements

The research of the third author was partially funded by ERC Starting Grant ANTICS 278537. The computations presented in this paper were carried out using the PlaFRIM experimental testbed (see `https://plafrim.bordeaux.inria.fr`). The authors would like to thank the anonymous referee for her/his helpful remarks that improved the presentation of the paper.

References

[1] E. Bayer, J.-P. Cerri, J. Chaubert, Euclidean minima and central division algebras, *Int. J. of Number Theory* **5** (2009), 1155–1168.

[2] J.-P. Cerri, Euclidean minima of totally real number fields: Algorithmic determination, *Math. Comput.* **76** (2007), 1547–1575.

[3] J.-P. Cerri, J. Chaubert, P.Lezowski, Euclidean totally definite quaternion fields over quadratic fields, *Int. J. of Number Theory* **9** (2013), 653–673.

[4] J. Chaubert, Minimum euclidien des ordres maximaux dans les algèbres centrales à division, PhD Thesis, EPFL (2006).

[5] M. Deuring, Algebren, Ergebnisse der Mathematik und ihrer Grenzgebiete, volume 4, Springer, (1935).

[6] M. Eichler, Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen, *J. Reine Angew. Math.* **179** (1938), 227–251.

[7] M. Harper, $\mathbb{Z}[\sqrt{14}]$ is Euclidean, *Can. J. Math.* **56** (2004), 55–70.

[8] P. Lezowski, Computation of the Euclidean Minimum of Algebraic Number Fields, *Math. Comp.* **83** (2014), 1397–1426.

[9] Magma, v2.19-5, Sydney, 2013, `http://magma.maths.usyd.edu.au/magma/`.

[10] I. Reiner, Maximal orders, Clarendon Press, Oxford, 2003.

[11] M.-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Math. 800, Springer, Berlin, 1980.